

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

- 5 1 (currently amended): A method for determining whether a
communication device is permitted to access communication
service in a communication network, the communication device
comprising:
- 10 a data memory capable of storing ciphertext access
information; and
an inerasable memory capable of storing a deciphering key in a
non-volatile way; and
the method comprising:
- 15 enciphering access information corresponding to the
communication device into the ciphertext access
information using a predetermined cryptography
algorithm according to an enciphering key, wherein
the enciphering key corresponds to the deciphering
key, and wherein the communication network comprises a
20 service provider capable of providing communication
service to the communication device; there being a
database in the service provider for recording the
enciphering key corresponding to the communication device;
and
- 25 recording the ciphertext access information in the data
memory;
reading the deciphering key in the inerasable memory and the
ciphertext access information in the data memory; and
deciphering the ciphertext access information to
30 plaintext access information according to the
deciphering key by using a ~~predetermined~~ the

cryptography algorithm, and determining whether the communication device is permitted to access communication service in the communication network accordingly.

5

2 (original): The method of claim 1 wherein the cryptography algorithm is an asymmetric encryption-and-decryption algorithm.

3 (original): The method of claim 1 wherein the data memory is a
10 non-volatile memory.

4 (cancelled)

5 (currently amended): The method of ~~claim 4~~ claim 1 further comprising:
15 generating the enciphering key and the corresponding deciphering key according to the cryptography algorithm before generating the ciphertext access information according to the enciphering key.

20 6 (cancelled)

7 (currently amended): The method of ~~claim 6~~ claim 1, wherein when generating the ciphertext access information according to the enciphering key, the service provider enciphers the access information corresponding to the
25 communication device to generate the ciphertext access information according to the enciphering key stored in the database.

8 (original): The method of claim 7, wherein when recording the ciphertext access information in the data memory, transmitting the
30 ciphertext access information from the service provider to the communication device via the communication network, and

recording the ciphertext access information in the data memory
with the communication device.

- 9 (currently amended): The method of ~~claim 4~~ claim 1, wherein the
5 enciphering key is different from the deciphering key.
- 10 (original): The method of claim 1, wherein when determining whether
the communication device is permitted to access communication
service of the communication network according to the plaintext
10 access information, determining whether the plaintext access
information conforms to predetermined access information; the
communication device being determined permitted to access the
communication service of the communication network if the
plaintext access information conforms to the predetermined
15 access information.
- 11 (original): The method of claim 1 in which the communication device
further comprises a subscriber identification module card (SIM
card) capable of recording a subscriber identification number, and
20 a predetermined identification number is recorded in the plaintext
access information, wherein when determining whether the
communication device is permitted to access communication
service in the communication network according to the plaintext
access information, determining whether the subscriber
25 identification code conforms to the predetermined identification
code; the communication device being permitted to access the
communication service if the predetermined identification code
and the subscriber identification code correspond to each other,
and the communication device being not permitted to access the
30 communication service and having access to the communication
network stopped if the predetermined identification code and the

subscriber identification code do not correspond to each other.

12 (currently amended): A communication device utilized in a
communication network for accessing communication service of
the communication network; the communication device
comprising:

a data memory capable of storing ciphertext access
information in a non-volatile way;

an inerasable memory capable of storing a deciphering key in a
non-volatile way; and

a processor capable of controlling operation of the communication
device;

wherein before the communication device accesses the communication service
of the communication network, the processor reads the deciphering key in the
inerasable memory and the ciphertext access information in the data memory,
utilizes a predetermined cryptography algorithm to decipher the ciphertext
access information to plaintext access information according to the
deciphering key, and determines whether the communication device is
permitted to access communication service of the communication network
according to plaintext access information;

wherein the communication network comprises a service provider for
providing communication service to the communication device;
there being a database in the service provider capable of recording the
enciphering key corresponding to the communication device; the ciphertext
access information being generated by enciphering the access
information corresponding to the communication device by the
cryptography algorithm according to the enciphering key, wherein
the enciphering key corresponds to the deciphering key.

13 (original): The communication device of claim 12 wherein the
cryptography algorithm is an asymmetric

encryption-and-decryption algorithm.

14 (cancelled)

5 15 (currently amended): The communication device of ~~claim 14~~
claim 12 wherein the enciphering key and the corresponding
deciphering key are generated according to the cryptography
algorithm.

10 16 (currently amended): The communication device of ~~claim 14~~
claim 12 wherein the ciphertext access information is transmitted
from the service provider to the communication device via the
communication network, and recorded in the data memory by the
communication device.

15

17 (original): The communication device of claim 12 wherein when
the processor determines whether the communication device is
permitted to access communication service according to the
plaintext access information, the processor determines whether
20 the plaintext access information conforms to predetermined
access information; wherein the processor determining the
communication device is permitted to access the communication
service if the plaintext access information conforms to the
predetermined access information.

25

18 (original): The communication device of claim 12 in which the
communication device further comprises a SIM card capable of
recording a subscriber identification number, and a predetermined
identification code is recorded in the plaintext access information,
30 wherein when the processor determines whether the
communication device is permitted to access communication

service according to the plaintext access information, the processor determines whether the subscriber identification code conforms to the predetermined identification code; the communication device being permitted to access the communication service if the predetermined identification code and the subscriber identification code correspond to each other, and the communication device being not permitted to access the communication service and access to the communication network being stopped if the predetermined identification code and the subscriber identification code do not correspond to each other.

19 (original): The communication device of claim 12 in which the communication device is a cell phone, and the communication network is a wireless communication network.

15

20 (currently amended): A method applied in a communication network, wherein the communication network comprises a plurality of communication devices and each communication device comprises an inerasable memory and a data memory; the method being capable of determining whether each communication device is permitted to access communication service of the communication network; the method comprising:

providing a plurality of different enciphering keys and a plurality of deciphering keys according to a cryptography algorithm, wherein each enciphering key corresponds to each deciphering key, wherein the communication network further comprises a service provider capable of transmitting signals and providing communication service among communication devices, service provider having a database storing enciphering keys corresponding to each communication device in the database;

30

providing different corresponding enciphering keys to different

communication devices;
enciphering access information corresponding to each
communication device to ciphertext access information
by the cryptography algorithm according to the
5 enciphering key corresponding to the communication
device;
storing deciphering keys corresponding to the enciphering
keys corresponding to each of the communication
devices in the inerasable memory;
10 storing ciphertext access information of each communication
device in the data memory of the communication device; and
when determining whether a communication device is
permitted to access the communication service,
deciphering the ciphertext access information in the
15 data memory by the cryptography algorithm according to
the enciphering key stored in the inerasable memory, and
determining whether the communication device is
permitted to access the communication service
according to the deciphered ciphertext access
20 information.

21 (original): The method of claim 20, wherein the deciphering keys
corresponding to different enciphering keys are different.

25 22 (original): The method of claim 20, wherein the cryptography
algorithm is an asymmetric encryption-and-decryption
algorithm such that an enciphering key is not equal to the
corresponding deciphering key, and when a plaintext is
enciphered into a ciphertext according to the enciphering key by
30 the cryptography algorithm, the cryptography algorithm cannot
decipher the ciphertext into the original plaintext according to

the enciphering key.

23 (cancelled)

- 5 24 (original): The method of claim 20 in which the communication device
is a cell phone, and the communication network is a wireless
communication network.